Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2009 Proceedings | Southern (SAIS)

3-1-2009

# Data Center Security: Analysis of Two Audit Reports

Ken Knapp
knappkj@gmail.com

Gary D. Denney

Mark E. Barner

# DATA CENTER SECURITY: ANALYSIS OF TWO AUDIT REPORTS

**Kenneth J. Knapp**
U. S. Air Force Academy
knappkj@gmail.com

**Gary D. Denney**
U. S. Air Force Academy

**Mark E. Barner**
U. S. Air Force Academy

## ABSTRACT

The increasing volume of electronic data, the need for secure storage of this data and the necessity for organizations to prepare for disaster are key reasons promoting the prominence of data centers in our society. Since data centers house large volumes of valuable information, proper security of organizational data centers is essential. This paper provides the reader with an overview of security principles relevant to data centers. We then offer a synopsis, aggregation and exploratory analysis of two audit reports of government data centers in the United States. We suggest general observations from the audit reports before concluding. As a contribution to the literature, this paper offers an investigative analysis of data center audits that can form a baseline for a more thorough future study on this relevant topic.

### Keywords

Data Center, Security, Audit Reports

## INTRODUCTION

In a style reminiscent of the 'wild west' days in the 19th century United States, two masked men allegedly pistol-whipped a lone IT staff worker during a graveyard shift, held the person hostage for two hours, while confiscating computer equipment in a Chicago data center (Thibodeau 2008). The burglars reportedly entered the facility through a fire escape, passing an unoccupied security guard post. The thieves waited in hiding for the IT staffer to leave the data center and then ambushed the staffer, subdued him, and swiped his card through a card reader and forced him to perform a finger print scan before stealing computer storage equipment. Since the incident, the company has hired armed guards to patrol the data center and its perimeter. Today, organizations must protect data centers much like banks. Banks utilize many forms of physical and operations security to include surveillance cameras, armed guards, accessible panic buttons and inner sanctums or vaults to protect the most valuable treasures of the bank. The bank analogy is sensible considering that modern societies are in what some call the digital age where information is a principal source of wealth and power. If this is the case, then data centers need protection much like that of the U. S. Bullion Depository at Fort Knox, Kentucky.

A data center is a central repository for the storage, management, and dissemination of data usually supporting a particular business or organization. Every organization with computers has some type of data center and every organization faces security threats to their data center. Smaller organizations may have their 'data center' stored on a single laptop or even consolidated onto a USB flash drive. Larger organizations may refer to a data center as a server room, server farm, computer room or a network operations center. Other organizations may have an internet data center, storage area network or network attached storage structures. The largest organizations often have multiple data centers located throughout the world. The above mentioned data storage configurations are different types of data centers where the major difference is the magnitude or storage capacity of the center.

Yet, it is not enough to say that data centers with sufficient storage capacity are necessary – data centers must also provide *secure* storage. Despite that cyber security is given more attention in the digital age, security breaches seem to continue unabated. One nonprofit consumer organization estimates there has been over 225 million records containing sensitive information involved in security breaches in the U. S. since January 2005 (Privacy Rights Clearinghouse 2008). Surprising is that nearly half of the compromises were not the work of devious network hacks or intruders, but direct data-storage losses such as the well known 2006 U. S. Veterans Administration loss of a laptop and storage device containing records on millions of veteran patients. At the same time, increasing amounts of sensitive data resulting from financial transactions, electronic health records, and large numbers of sensors is

substantially escalating the need to store sensitive data. Moreover, organizations often locate data centers in different geographic regions to mitigate risk and provide a business continuity capability in the event of a disaster at a single location resulting from a terrorist attack, hurricane or earthquake. It is clear that organizations today need efficient and affordable data storage facilities that are also secure, reliable and available.

The notion of defense-in-depth is a valuable security approach and stipulates that security should be multi-layered and that security processes should penetrate deep into an organization; layers of security offer both redundancy and diversity to help protect the system from threats. Defense-in-depth is receiving greater acceptance as a model for IT security and has been specifically applied to the security of many modern data centers (Santos 2007). Practically, when building a data center facility, defense-in-depth security considerations need to be built into the very design philosophy of the structure. In a recent data center project, Terremark Worldwide constructed a 50,000-square foot facility using a tiered approach. For its most sensitive systems, there are seven layers of physical security before a person can physically even touch a computer. These layers consist of a variety of security devices to include biometrics, gates, fences, guards, identity cards and even ditches and hills. Some of the gates and fencing are rated strong enough to stop a truck moving at 35 miles per hour. Another organization anonymously reported building what seemed to be a simple retention wall 3 feet high around its data center. But in reality, the wall extended 9 feet underground with steel reinforcement built to withstand a 60 mile per hour hit from an 18 wheel truck loaded with explosives. Other organizations, such as Deutsche Bank and Continental Airlines, house data centers and backup facilities in highly protected underground bunkers (Hoover 2008).

An objective of this paper is to provide readers with a useful overview of security principles and issues of data centers drawn primarily from the practitioner literature. Baskerville & Myers (2004, p. 329) state that there have been, "frequent calls for IS researchers to make their research more relevant to practice (Zmud 1998), yet it seems IS researchers continue to struggle to make excellent research practically relevant." In this conference paper, heeding calls to offer more relevant IS research, we offer an exploratory analysis of data center audits that can form a baseline for a more thorough future study on this pertinent topic. To our knowledge, no published academic study exists that aggregates results across multiple data center audits. Having introduced the topic, we now analyze two audit reports of government data centers in the U. S. We then summarize the audit reports and offer general observations.

## ANALYSIS: TWO DATA CENTER AUDITS

To understand the types of security issues that data centers face, the authors analyzed two publicly available reports detailing the results of data center audits. Audits are conducted to help ensure a data center has adequate physical, cyber, environmental, and managerial security controls in place to prevent security incidents and thus protect the data resource. Data center audits may be done for a variety of reasons to include compliance with applicable laws or per internal organizational policy. If professionally accomplished, audits highlight security weaknesses and offer practical remedies to improve data center security. Analyzing audit reports can be valuable since they summarize the essential concerns and challenges facing data center operations and security. We will first discuss audit methodologies before covering the two cases.

## AUDIT METHODOLOGIES

It is important that experienced specialists conduct data center audits. Professional certifications such as the broad-based Certified Information Systems Security Professional (CISSP) or the more audit-focused Certified Information Systems Auditor (CISA) add credentials to the data center auditor. Data collection for data center audits typically emanate from a number of sources. Here, we list six potential sources. First, auditors can assess security through observation to include site survey and facility tours. Second, auditors can talk to data center workers through formal interviews or from spot questions made during facility observation. Third, automated tools are available to test important network systems such as firewalls and access control systems. Fourth, auditors can review access control records to include facility access logs and system accounts. Fifth, auditors may directly test (although often in a limited fashion) critical systems such as fire suppression systems or backup power supplies. Sixth, auditors may also review management documents such as disaster recovery plans, security training programs or support-level agreements. Overall, inspectors should not rush data center audits; they can take as little time as one day or extend for months. After the audit, data center management should follow-up with progress reports documenting 'get well' plans as well as the actions taken to correct identified security weaknesses.

Following are summaries of two data center audits of United States government organizations. The first author accessed each audit report through the public internet. For each audit case, a background is provided and a summary of the findings. The first audit was conducted at the U. S. federal government level in 1996 and offers a historical perspective of a data center audit. The second was conducted in the U. S. at the state level in 2006. We then present an analysis of the two cases to include classifying all audit findings into one of the information security Common Body of Knowledge (CBK) categories. Finally, we offer general observations from the two cases.

**Case #1: Internal Revenue Service 'Cyberfile' Data Center Review (1996)**

The Internal Revenue Service (IRS) is the United States federal government agency that collects taxes and enforces internal revenue laws. As such, the IRS is a very information intensive organization that relies heavily on technology to accomplish its mission. On March 12, 1996, the United States General Accounting Office (GAO) conducted a review of an IRS data center. This data center was a $17 million project (1996 dollars) for supporting a new electronic filing system called Cyberfile. The GAO auditors understood that this data center was to go into production on March 19, 1996 and conducted the audit one week prior to production. The audit identified 49 weaknesses across seven categories including data center operations, physical security, data communications management, disaster recovery, contingency planning, risk analysis, and security awareness (GAO 1996).

Of the 49 specific findings, some were temporary issues such identifying the need to remove combustible materials outside the data center. Other issues were structural in nature such as highlighting that the data center is located on a subbasement level of a building without water detectors under the raised floor.

The IRS highly contested the GAO audit report which listed many serious security weaknesses. First, the IRS contested that the operational date of March 19, 1996 as understood by the GAO was incorrect. In their reply to the GAO audit, the IRS stated that on March 1, 1996, 12 days prior to the GAO audit, the IRS executive committee and external partners were notified that the Cyberfile data center would not be in production as initially planned. Secondly, the IRS contested many of the findings as inherent to a non-production data center under construction, such as the first finding about large amounts of combustible material inside the data center. While the possible miscommunication between the GAO and the IRS was unfortunate, the IRS did acknowledge and address a number of potentially serious security weaknesses. For example, regarding the lack of water detectors under the raised floor, the IRS developed a proposal for the deployment of such technology the month following the review.

The Cyberfile data center case provides a noteworthy and historical case study in how a contentious data center audit can still deliver positive results. Although dated to 1996, the findings offer lessons that are still valuable for today's data center: many of the problems experienced with this case remain relevant today. The Cyberfile review was a high visibility review; the GAO addressed the report to a U. S. Senator and the IRS received negative media attention because of the report. While it is unfair to apply production-level security to a developmental data center, in our analysis, a large number of the 49 findings were legitimate regardless of the production status. The IRS quickly responded to the GAO review by claiming to have corrected 32 of the 49 weaknesses within six weeks of the review with plans to correct the remaining weaknesses prior to full production. However, the security problems at the data center may have been predictive of additional problems with the Cyberfile system; six months after the GAO data center audit, the IRS scrapped the Cyberfile system altogether (Chandler 1996). In the end analysis, the 49 findings (see GAO 1996) from the audit provide a worthwhile study of how *not* to build a data center. We believe the findings are comprehensive enough to be used as a type of checklist of problems to avoid in data center design and construction.

**Case #2: Montana Department of Administration Data Center Security Audit (2006)**

The second case involves a 2006 data center audit of the State of Montana's Department of Administration (DofA). The DofA maintains a data center as a service to state agencies that stores data relating to accounting, budgeting, human resources, revenue, and public health and human services. The total value of the data center equipment was estimated at $14 million (2006 dollars). The focus of the audit was on the management and protection of the data center against physical, logical, and environmental threats. The scope of the audit included the entire data center and all of the resources within it, but did not include access controls related to any particular information system and excluded network devices such as firewalls (Seacat 2006; Stout 2007).

The audit methodology included interviews with agency personnel, walkthroughs and inspections of the facilities, observations, and reviews of documentation and equipment configurations. The auditors referred to ISACA's Objectives for Information Technology and Control Practices, the Federal Information Systems Control and Audit Manual, as well as statewide IT policies. Overall, the auditors cited the DofA for not having processes in place to ensure data center operations continuity and for the lack of management controls in the decision making process.

The DofA audit report stated that the data center focused on providing services to other agencies. However, arguing that since DofA houses some of the most sensitive data in state government (e.g. revenue related), the operational philosophy of the center should side toward security. Additionally, the auditors found that multiple agencies are responsible for different aspects of security. For example, one agency was responsible for network security and another for physical security. The report stated, "The overlapping areas of responsibility created barriers to security efforts due to conflicting priorities. The department does not have somebody responsible for the data center as a whole, and for coordinating efforts to ensure security of the data center" (Seacat 2006, p.14).

The audit report contained fifteen specific recommendations for security improvement. In their response to the audit, while recognizing the seriousness of many of the findings, DofA concurred with all fifteen recommendations and assigned target dates for each recommendation related action. Although not as grave as the IRS Cyberfile audit findings, Montana's Department of Administration finding was nevertheless critical of the state of security at the data center. Also in contrast to the IRS case, the overall tone of the audit process from both sides appeared constructive and appreciative. A year after the June 2006 report, the auditor released a memorandum that detailed progress the DofA had made toward fixing deficiencies. However, a year after the June 2006 report, of the fifteen specific recommendations, only one was considered 'implemented' with thirteen considered 'partially implemented' and one recommendation 'not implemented' (Stout 2007). In one finding, the audit report recommended to "conduct a cost analysis associated with implementing or improving controls." The DofA concurred and stated that a "cost analysis will be conducted" based on a threat analysis with an estimated completion date of August 31, 2006. By June 2007, however, the department completed the cost analysis but not the threat analysis.

## SUMMARY ANALYSIS OF THE AUDITS

The two audit reports documented 64 total findings. Taking an exploratory approach to classifying each of the findings in the two audit reports, we searched for a framework that incorporates the broad range of security threats facing data centers today. The information security common body of knowledge (CBK) served this purpose. The International Information Systems Security Certification Consortium [$(ISC)^2$] is a non-profit organization that manages the CBK and the certified information system security professional (CISSP) program.[1] The CISSP is the first IT certification to be accredited under ISO/IEC 17024, a global benchmark for the certification of workers in various professions (Vijayan 2004). This ISO certification adds credibility and validity to the $(ISC)^2$ organization as one of the world's foremost certifying bodies. Established in 1989, the CBK has provided a shared reference for information security professionals. Described on the $(ISC)^2$ web site, "the $(ISC)^2$ CBK is a taxonomy - a collection of topics relevant to information security professionals around the world…(it) establishes a common framework of information security terms and principles which allows information security professionals worldwide to discuss, debate, and resolve matters pertaining to the profession with a common understanding."

The authors selected the CBK model over other security models (e.g. the CIA triad) because of its comprehensive and practical orientation. Rather than being an academic framework, the CBK is inherently practitioner oriented and at a suitable level for classifying real-world security issues. During our analysis, we classified each of the 64 audit findings into one of the ten categories of the CBK. Table 1 summarizes our results by providing a numerical tally of the audit findings from the two cases categorized by the CBK.[2]

| CBK Category | IRS Cyberfile | Montana DOA | Totals | Percent |
|---|---|---|---|---|
| Information Security Management | 5 | 6 | 11 | 17% |
| Security Architecture | 0 | 0 | 0 | 0% |
| Access Control | 9 | 4 | 13 | 20% |
| Application Security | 1 | 0 | 1 | 2% |
| Operations Security | 16 | 0 | 16 | 25% |
| Cryptography | 0 | 0 | 0 | 0% |

| | | | | |
|---|---|---|---|---|
| Physical Security | 7 | 2 | 9 | 14% |
| Telecommunications/Networks | 7 | 0 | 7 | 11% |
| Business Continuity Planning | 4 | 3 | 7 | 11% |
| Law, Investigations, Ethics | 0 | 0 | 0 | 0% |
| Totals | 49 | 15 | 64 | 100% |

**Table 1. Summary of Audit Findings Classified by the CBK**

Based on our review of the literature, no prior study exists that aggregates results across multiple data center audits. Thus, the contribution of this study is that it might be the first of its kind in the academic literature. Additionally, much of the discussion of this study has focused on operations and physical security, areas previously identified as lacking in the information systems literature (Knapp et al. 2007). However, our selected categorization approach has both strengths and limitations. As a strength, the information security CBK is a widely used industry framework and at the appropriate level for the categorization purposes of this study. In addition, both audit reports already categorized their findings using a naming convention similar to that of the CBK, making categorization of the findings somewhat straightforward. As a limitation, some of the findings that overlapped CBK domains could have been classified in multiple domains. The most difficult categorization related to findings that overlapped the *access control* and *physical security* domains. We resolved the overlap by deciding that access control related findings pertaining to the physical structure we categorized as *physical security* and access control related findings pertaining to procedures and logic we categorized under *access control*. Overall, we selected the closest CBK category based on the writing emphasis of the audit finding. Finally, we consider our research study clearly to be exploratory since we analyzed only two audit case studies. Thus, we cannot generalize our results or suggest that our study contains cases that are representative of typical data center audits. This is especially the situation for the Montana audit, for example, where auditors considered computer applications, databases and network devices to be outside of the audit scope.

## OBSERVATIONS FROM THE AUDITS REPORTS

From analyzing the audit reports, it is clear that data center issues go well beyond network and computer security. Instead, the issues range in varying degrees across CBK domain topics. The top four categories representing 76% of the findings are Operations security (25%), Access control (20%), Security management (17%) and Physical Security (14%).

It should not be surprising that *operations security* and *access control* related findings received the most attention in the audit reports. Pertaining to data centers, operations security identifies the controls over the hardware, media, and the personnel who have the access privileges to the center. It addresses the protection of data center assets while the data is resident in storage devices or in transit across networks in and out of the center. Others have argued that operations security is the heart of information security since it controls the way data is accessed and processed (Fisher 1999). In data centers, this may especially be the case. In the audit reports, operations security-related issues ranged from daily facility procedures to personnel safety concerns, which were especially evident in the IRS audit. Twenty percent of the findings were in the *access control* category. This domain outlines various security options that control access to an organization's information and data processing resources. It builds on the basic issues addressed in the information security management category with an emphasis on administrative, physical, and logical controls (Hansche et al. 2004). In the audit reports, access control issues typically pertained to individual access to data center resources such as taking actions that will minimize the likelihood of unauthorized personnel entering the data center.

The domain categories of *information security management* and *physical security* also received significant attention in the audit reports. We could argue that every finding is ultimately a management responsibility to a certain degree. Yet, a number of findings are significant management issues. In the Montana DofA report, the auditors recommended that the "department clearly define and designate responsibility…of all aspects of security." This is a major finding in that important responsibilities were divided among groups in different organizations. For example, physical security was the responsibility of one organization while network security the responsibility of another. This structure "created barriers to security efforts…the department does not have somebody responsible for the data center as a whole" (Seacat 2006, p. 15). Considering the importance of data centers today, it can be considered a best practice to have a single organization or person responsible for the data center overall. In the domain of

physical security, both audit reports identified weaknesses with perimeter security (which is both a physical security and access control issue). The IRS report stated that the "data center did not have a secure perimeter. Access to shared areas that completely encircle the data center was not controlled" by the data center. The Montana DofA report identified similar problems. The data center, which also was located in a shared building, did not have walls extended to the true ceiling and the office responsible for physical security was not aware of this vulnerability. This was an important finding in both reports in that perimeter defense is a fundamental aspect of data center security.

Three of the CBK categories did not have any audit findings classified in them: *cryptography*, *security architecture* and *law, investigations and ethics*. However, it would be incorrect to conclude that these categories are not relevant to the security of data centers. Cryptography, for example, is particularly important when sensitive data travels over a network. Confidential or restricted telecommunications traffic going in and out of the data center should be encrypted. Some laws, such as HIPAA, specifically require certain types of personnel health information to be encrypted at least during transmission (HHS 2008). Additionally, encrypting data in storage is prudent especially sensitive information such as medical or financial records. Investigating and auditing encryption concerns in data centers may require an auditor who specializes in cryptography issues.

## CONCLUSION

In this paper, we provided the reader with an overview of security principles and issues relevant to data centers. We then offered a synopsis and exploratory analysis of two audit reports of government data centers in the United States before making general observations. This paper offers an investigative analysis of data center audits that can form a baseline for a more thorough future study on this relevant topic. Since data centers house large volumes of valuable information, proper security of data centers is essential. We trust that the reader has a better understating of the security issues facing modern data centers.

## REFERENCES

1. Baskerville, R.L., and Myers, M.D. "Special Issue on Action Research in Information Systems: Making IS Research Relevant to Practice. Forward," *MIS Quarterly* (28:3), September 2004, pp 329-335.
2. Chandler, C. "The Agency They Love to Get Excised About - IRS's Own Problems and a Complex Tax Code Make It a Favorite Political Target This Year," in: *The Washington Post*, Washington D. C., 1996, p. H1.
3. Fisher, P. "Operations Security and Controls," in: *Information Security Management Handbook*, H.F. Tipton and M. Krause (eds.), Auerbach Publications, Boca Raton, FL, 1999, p. 699.
4. GAO "GAO/AIMD-96-85r Security Weaknesses at IRS' Cyberfile Data Center," General Accounting Office, Accounting and Information Management Division, Washington D. C., p. 21.
5. Hansche, S., Berti, J., and Hare, C. *Official (ISC)$^2$ Guide to the CISSP Exam* Auerbach, New York, 2004.
6. HHS "Department of Health & Human Services HIPAA Security Guidance," U.S.D.o. HH&S (ed.), 2008.
7. Hoover, N. "Data Center Best Practices," in: *Information Week*, 2008.
8. Knapp, K.J., Ford, F.N., Marshall, T.E., and Rainer, K.R.J. "The Common Body of Knowledge: A Framework to Promote Relevant Information Security Research," *Journal of Digital Forensics, Security, and Law* (2:1) 2007, pp 9-34.
9. Privacy Rights Clearinghouse "A Chronology of Data Breaches," 2008.
10. Santos, O. *End-to-End Network Security: Defense-in-Depth* Cisco Press, 2007, p. 400.
11. Seacat, S.A. "Data Center Review, Department of Administration," Legislative Audit Division, State of Montana, Helena, MT, p. 24.
12. Stout, D. "Memorandum. Re: Department of Administration, IS Audit Data Center Review Follow-up 07sp-025 (Orig. 06dp-05)," Legislative Audit Division, Helena, MT, p. 6.
13. Thibodeau, P. "Robbery Alters Thinking on Data Center Security," in: *ComputerWorld*, 2008.
14. Vijayan, J. "ISO Endorses Key Security Certification," in: *ComputerWorld*, 2004, pp. 1-2.
15. Zmud, R. "Editor's Comments," *MIS Quarterly* (22:2) 1998, pp xxxix-xxxii.

[1] *(ISC)$^2$*, *CISSP*, and the *Common Body of Knowledge (CBK)* are registered marks. See www.isc2.org. . In the practitioner literature, we have seen the CBK interchangeably referred to as the CISSP CBK, the (ISC)$^2$ CBK, and the information security CBK.

[2] An appendix containing the extended analysis and classification is available from the first author upon request.